CLAIMS

1. In a method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity.

by means of all or part of the following parameters or derivatives of these parameters:

- a public modulus **n** constituted by the product of **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being equal to or greater than 2),

- a public exponent **v**;

- **m** distinct integer base numbers $g_1, g_2, \ldots g_m$ (**m** being greater than or equal to 1), the base numbers g_i being such that:

the two equations (1) and (2):

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

cannot be resolved in x in a ring of integers modulo **n**,

and such that:

the equation (3):

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of integers modulo **n**.

the method according to the invention making it possible to produce the **f** prime factors $p_1, p_2, \ldots p_f$ in such a way that the equations (1), (2) and (3) are satisfied, said method comprising the step of choosing firstly:

- the **m** base numbers $g_1, g_2, \ldots g_m$,
- the size of the modulus **n**,
- the size of the **f** prime factors $p_1, p_2, \ldots p_f$.

2. Method according to claim 1 such that, when the public exponent **v** has the form:

$$v = 2^k$$

where **k** is a security parameter greater than 1, the security parameter **k** is

also chosen as a prime number.

3. Method according to one of the claims 1 or 2, such that the **m** base numbers $g_{1,}, g_{2,}, \ldots g_m$, are chosen at least partly among the first integers.

4. Method according to one of the claims 2 or 3, such that the security parameter **k** is a small integer, especially smaller than 100.

5. Method according to one of the claims 1 to 4, such that the size of the modulus **n** is greater than several hundreds of bits.

6. Method according to one of the claims 1 to 5, such that the **f** prime factors $p_{1,}, p_{2,}, \ldots p_f$ have a size close to the size of the modulus **n** divided by the number **f** of factors..

7. Method according to one of the claims 1 to 6 such that, among the **f** prime factors $p_{1,}, p_{2,}, \ldots p_f$,

- a number **e** of prime factors congruent to 1 modulo 4 is chosen, e possibly being zero (should **e** be zero, the modulus **n** will hereinafter be called a basic modulus, should **e > 0**, the modulus **n** will hereinafter be called a combined modulus),

- the **f-e** other prime factors are chosen to be congruent to 3 modulo 4, **f-e** being at least equal to 2.

8. A method according to claim 7 such that, to produce the **f-e** prime factors $p_{1,}, p_{2,}, \ldots p_{f-e}$ congruent to 3 modulo 4, the following steps are implemented:

- the first prime factor p_1 congruent to 3 modulo 4 is chosen and then,

- the second prime factor p_2 is chosen such that p_2 is complementary to p_1 with respect to the base number g_1.

- the factor p_{i+1} is chosen in carrying out the following procedure in, distinguishing two cases:

(1) the case where i> m

- the factor p_{i+1} congruent to 3 modulo 4 is chosen.

(2) Case where i≤m

- the Profile ($\mathbf{Profile_i(g_i)}$) of $\mathbf{g_i}$ with respect to the i first prime factors $\mathbf{p_i}$ is computed:

- if the $\mathbf{Profile_i(g_i)}$ is flat, the factor $\mathbf{p_{i+1}}$ is chosen such that $\mathbf{p_{i+1}}$ is complementary to $\mathbf{p_1}$ with respect to $\mathbf{g_i}$,

- else, among the **i-1** base numbers $\mathbf{g_1, g_2, \ldots g_{i-1}}$ and all their multiplicative combinations, the number, hereinafter called **g**, is chosen such that $\mathbf{Profile_i(g) = Profile_i(g_i)}$, and then $\mathbf{p_{i+1}}$ is chosen such that $\mathbf{Profile_{i+1}(g_i) \neq Profile_{i+1}(g)}$.

(the terms "complementary", "profile", "flat profile" having the meanings defined in the description).

9. A method according to claim 8 such that, to choose the last prime factor $\mathbf{p_{f-e}}$, the following procedure is used in distinguishing three cases:

(1) Case where f-e-1 > m

• $\mathbf{p_{f-e}}$ is chosen congruent to 3 modulo 4.

(2) Case where f-e-1 = m

• $\mathbf{Profile_{f-e-1}(g_m)}$ is computed with respect to the f-e-1 first prime factors from, $\mathbf{p_1}$ to $\mathbf{p_{f-e-1}}$,

• • if $\mathbf{Profile_{f-e-1}(g_m)}$ is flat, $\mathbf{p_{f-e-1}}$ is chosen such that it is complementary to $\mathbf{p_1}$ with respect to $\mathbf{g_m}$,

• • else:

• • • among the **m-1** base numbers from $\mathbf{g_1}$ to $\mathbf{g_{m-1}}$ and all their multiplicative combinations, the number hereinafter called **g** is chosen such that $\mathbf{Profile_i(g) = Profile_i(g_i)}$,

• • • then $\mathbf{p_{f-e}}$ is chosen such that $\mathbf{Profile_{f-e}(g) \neq Profile_{f-e}(g_m)}$.

(3) Case where f-e-1 < m

• $\mathbf{p_{f-e}}$ is chosen such that the following two conditions are met:

(3.1) First condition

• $\mathbf{Profile_{f\text{-}e\text{-}1}(g_{f\text{-}e\text{-}1})}$ is computed with respect to the f-e-1 first prime factors from $\mathbf{p_1}$ to $\mathbf{p_{f\text{-}e\text{-}1}}$,

• • If $\mathbf{Profile_{f\text{-}e\text{-}1}(g_{f\text{-}e\text{-}1})}$ is flat, $\mathbf{p_{f\text{-}e}}$ is chosen so that it meets the first condition of being complementary to $\mathbf{p_1}$ with respect to $g_{f\text{-}e\text{-}1}$.

• • Else,

• • • among the **f-e-1** base numbers from g_1 to $\mathbf{g_{m\text{-}1}}$ and all their multiplicative combinations, the number, hereinafter called **g** is chosen such that $\mathbf{Profile_i(g)} = \mathbf{Profile_{f\text{-}e\text{-}1}(g_{f\text{-}e\text{-}1})}$,

• • • then $\mathbf{p_{f\text{-}e}}$ is chosen so that it meets the first condition of being such that $\mathbf{Profile_{f\text{-}e}\ (g) \neq Profile_{f\text{-}e}\ (g_m)}$,

(3.2) Second condition

• among all the last base numbers from $\mathbf{g_{f\text{-}e}}$ to $\mathbf{g_m}$, those numbers whose Profile $\mathbf{Profile_{f\text{-}e\text{-}1}(g_i)}$ is flat are chosen and then

• $\mathbf{p_{f\text{-}e}}$ is chosen so that it meets the second condition of being complementary to $\mathbf{p_1}$ with respect to each of the base numbers thus selected.

10. Method according to the claims 8 or 9 such that, to produce the **e** prime factors congruent to 1 modulo 4, each prime factor candidate **p** is evaluated, from $\mathbf{p_{f\text{-}e}}$ to $\mathbf{p_f}$, in being subjected to the following two successive tests:

(1) First test

- the Legendre symbol is computed for each base number $\mathbf{g_i}$, from $\mathbf{g_1}$ to $\mathbf{g_m}$, with respect to the candidate prime factor **p**,

• if the Legendre symbol is equal to –1, the candidate **p** is rejected,

• if the Legendre symbol is equal to +1, the evaluation of the candidate **p** is continued in passing to the following base

number and then, when the last base number has been taken into account, there is a passage to the second test.

(2) Second test

- an integer number **t** is computed such that p-1 is divisible by 2^t, but not by 2^{t+1}, then

- an integer **s** is computed such that **s = $(p-1+2^t)/2^{t+1}$.**

- the key **⟨s, p⟩** is applied to each public value **G_i** to obtain a result **r**

$$\mathbf{r \equiv G_i^{\,s} \bmod p}$$

• if **r** is equal to **g_i** or - **g_i**, the second test is continued in passing to the following public value **G_{i+1}**.

• if **r** is different from **g_i** or - **g_i**, a factor **u** is computed in applying the following algorithm:

• • the algorithm consists of the repetition of the following sequence specified for an index **ii** ranging from 1 to t-2:

• • the algorithm implements two variables: **w** initialized by **r** and **jj** = 2^{ii} assuming values ranging from 2 to 2^{t-2}, as well a number **b** obtained by application of the key **⟨(p-1)/2^t, p⟩** to a non-quadratic residue of CG(p), then the following steps 1 and 2 are iterated:

• • • Step 1: w^2/G_i (mod p) is computed,

• • • Step 2: the result is raised to the power of 2^{t-ii-1}.

• • • • If +1 is obtained, the second test is continued in passing to the following public value G_{i+1},

• • • • If –1 is obtained, jj = 2^{ii} is computed and then w is replaced by w.b^{jj} (mod p), then the algorithm is continued for the following value having an index ii.

• • at the end of the algorithm, the value in the variable jj is used to compute an integer u by the relation $jj = 2^{t-u}$ and then the expression t-u is computed. Two cases arise:

• • • if t-u < k, the candidate **p** is rejected

• • • if t-u > k, the evaluation of the candidate **p** is continued in continuing the second test and in passing to the following public value $G_{i+1,}$ the candidate **p** is accepted as a prime factor congruent to 1 modulo 4 if, at the end of the second test, for all the **m** public values G_i, it has not been rejected.

11. Method applying the method according to any of the claims 1 to 10, making it possible to produce **f** prime factors $p_{1,}$, $p_{2,}$, ... p_f , this method being designed to prove the following to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ (**m** being greater than or equal to 1),
- the public modulus **n** constituted by the product of said prime factors **f** $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),
- the public exponent **v**;

said modulus, said exponent and said values being linked by relations of the following type:

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^v \bmod n .$$

said exponent **v** being such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

said public value G_i being the square g_i^2 of the base number g_i smaller than

the **f** prime factors $p_1, p_2, \dots p_f$, the base number g_i being such that: the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

cannot be resolved in x in the ring of integers modulo **n** and such that: the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n.**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or of the public modulus **n** and/or the **m** private values Q_i and/or **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v**;

- the witness computes commitments **R** in the ring of integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random factor such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random factors $\{r_1, r_2, \dots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d**, comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computing a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \dots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \, . \, Q_{i,1}{}^{d1} \, . \, Q_{i,2}{}^{d2} . \ldots Q_{i,m}{}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method.

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

12. A method according to claim 11 such that to implement the pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ as just described, the method uses the prime factors $p_1, p_2, \ldots p_f$ and/or the parameters of the Chinese remainders, the base numbers $g_1, g_2, \ldots g_m$ and/or the public values $G_1, G_2, \ldots G_m$ to compute:

- either the private values $Q_1, Q_2, \ldots Q_m$ by extracting a **k-th** square root modulo **n** of G_i, or by taking the inverse of a **k-th** square root modulo **n** of G_i,

- or the **f.m** private components $Q_{i,j}$ of the private values $Q_1, Q_2, \ldots Q_m$ such that $Q_{i,j} \equiv Q_i \pmod{p_j}$.

13. A method according to claim 12 such that,to compute the **f.m** private components $Q_{i,j}$ of the private values $Q_1, Q_2, \ldots Q_m$:

- the key $\langle s, p_j \rangle$ is applied to compute **z** such that:

$$z \equiv G_i^{\,s} \pmod{p_j}$$

- and the values **t** and **u** are used.

- computed as indicated here above when p_j is congruent to 1 modulo 4 and

• taken to be respectively equal to 1 (t=1) and 0 (u=0) where p_j is congruent to 3 modulo 4.

• • if **u** is zero, we consider all the numbers zz such that:

• • • zz is equal to z or such that

• • • zz is equal to a product (mod p_j) of z by each of

the 2^{ii-t} 2^{ii}-th primitive roots of unity, ii ranging from 1 to min(k,t).

• • If **u** is positive, we consider all the numbers zz such that zz is equal to the product (mod p_j) of za by each of the 2^k 2^k-th roots of unity, za designating the value of the variable w at the end of the algorithm implemented in claim 10,

- at least one value of the component $\mathbf{Q_{i,j}}$ is deduced therefrom, it is equal to zz when the equation $\mathbf{G_i \equiv Q_i^v \bmod n}$ is used or else it is equal to the inverse of zz modulo p_j of zz when the equation $\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot \bmod n}$ is used.